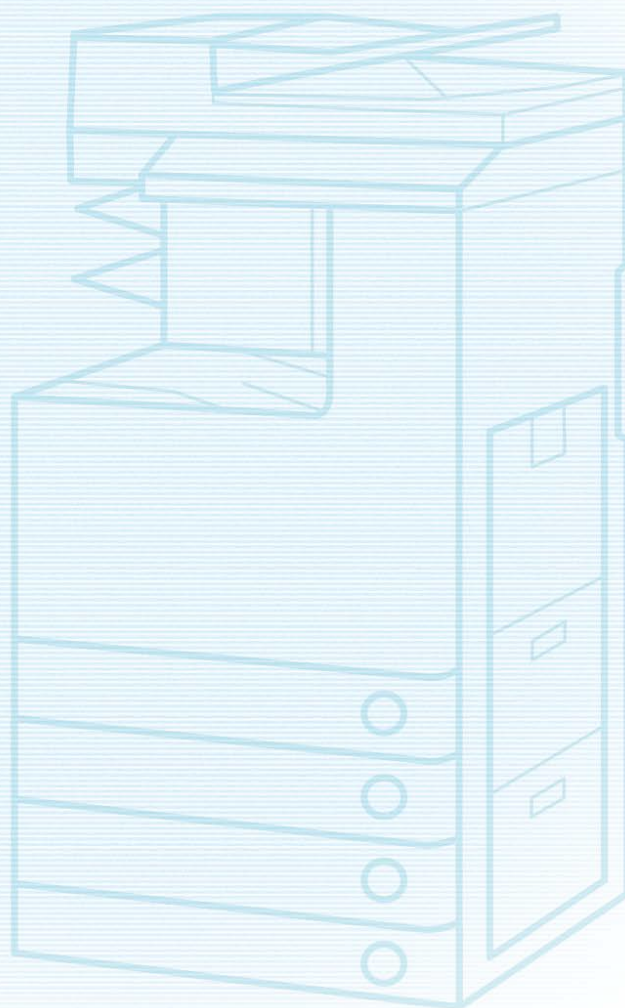
オフィス向け複合機（iR-ADV ／ iRC ／ iR シリーズ）
プロダクション向け複合機（iR-ADV PRO ／ imagePRESS シリーズ）
不正アクセス防止対策について

重要　管理者の方は、必ずご一読ください。

平素より、キヤノン製品をご愛顧いただき、誠にありがとうございます。本文書ではオフィス向け複合機（iR-ADV ／ iRC ／ iR シリーズ）ならびにプロダクション向け複合機（iR-ADV PRO ／ imagePRESS シリーズ）（※以降、複合機）における外部ネットワークからの不正アクセス防止対策を取扱説明書の要約として記載いたします。管理者の方は、必ずご一読いただけますよう、よろしくお願い申し上げます。なお、オプションのimagePRESS Server ／ ColorPASS ／ imagePASSについては、各製品の取扱説明書を参照してください。imagePRESS C7011VPSについては、「PRISMAsyncコントローラーのセキュリティに関して」を参照してください。

はじめに

近年の複合機は多機能化が進み、従来のコピーやファクス、プリントといった機能に加え、ネットワーク経由での各種プロトコルによるアクセスを前提とした機能が多数搭載されるようになりました。キヤノンの複合機においても例外ではなく、HTTPプロトコルによるリモートUI、SMB ／ WebDAVプロトコルなどによるファイル共有など、さまざまな便利な機能が利用できるようになっています。以降では、キヤノンの複合機における、外部からの不正アクセス対策のポイントを紹介していきます。

外部からの不正アクセス対策のポイント

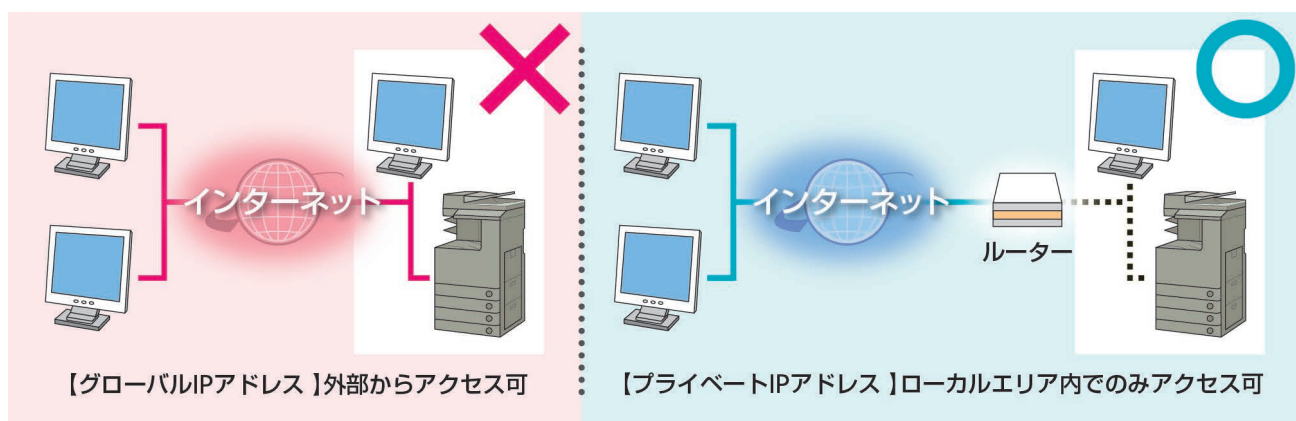
1. **プライベートIPアドレスで運用する**
2. **ファイアウォールで通信を制限する**
3. **複合機が持つ情報をパスワードで管理する**
4. **リモートUIの使用を制限する**
5. **SSL暗号化通信を設定する**

プライベート IP アドレスで運用する

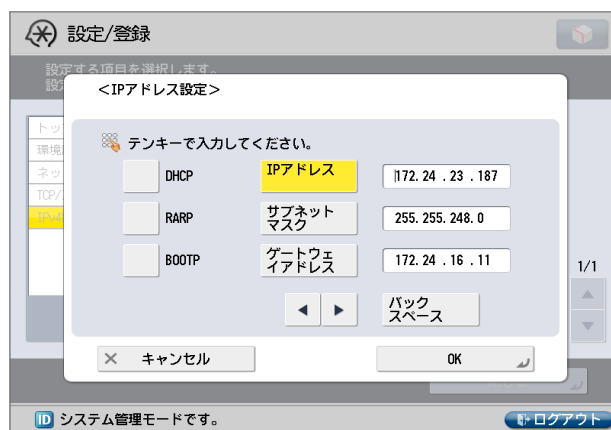
IPアドレスとは、ネットワーク上の機器に割り当てられる番号のことで、インターネット接続に使われるIPアドレスを**「グローバルIPアドレス」**社内LANなどのローカルエリアネットワークで使われるIPアドレスを**「プライベートIPアドレス」**と呼びます。複合機に設定されているIPアドレスがグローバルIPアドレスの場合は、インターネット上の不特定多数のユーザーからアクセス可能な状態であり、外部からの不正アクセスによる情報漏えいなどのリスクも高まります。一方で、プライベートIPアドレスが設定されている複合機なら、社内LANなどのローカルエリアネットワーク上のユーザーからしかアクセスすることができません。

基本的には、複合機のIPアドレスにはプライベートIPアドレスを設定して運用してください。プライベートIPアドレスには、以下のいずれかの範囲のアドレスが使用されます。お使いの複合機に設定されているIPアドレスがプライベートIPアドレスかどうかを確認するようにしてください。

プライベートIPアドレスの範囲

・10.0.0.0 ～ 10.255.255.255
・172.16.0.0 ～ 172.31.255.255
・192.168.0.0 ～ 192.168.255.255

MEMO

複合機にグローバルIPアドレスが設定されていても、ファイアウォール等で外部からのアクセスを防御する環境を構築すれば、不正アクセスのリスクは軽減されます。複合機にグローバルIPアドレスを設定して運用したいときは、社内のネットワーク管理者にご相談ください。

■ iR-ADV ／ 一部の imagePRESS シリーズでの IP アドレスの確認

※ IP アドレスの確認手順については、本体同梱の取扱説明書を参照してください。

■ iRC ／ iR ／ imagePRESS シリーズでの IP アドレスの確認

※ IP アドレスの確認手順については、本体同梱の取扱説明書を参照してください。

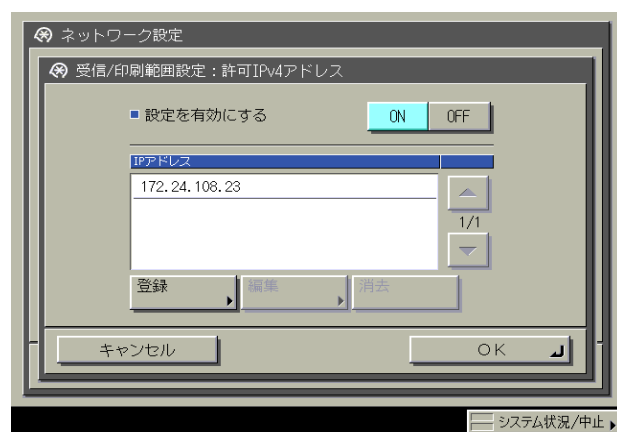
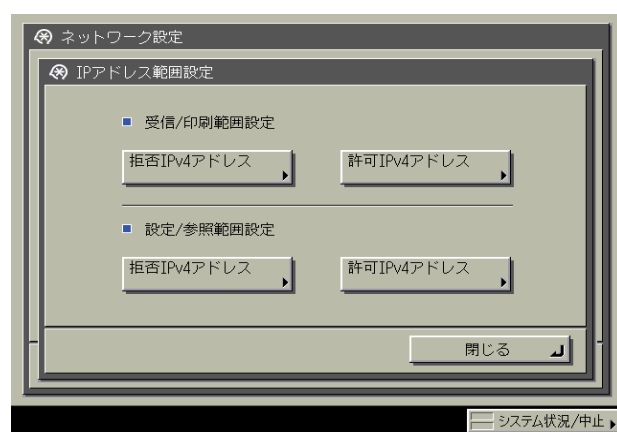
ファイアウォールで通信を制限する

ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、組織内のネットワークへの攻撃や侵入を防ぐシステムです。キヤノンの複合機に搭載したファイアウォールを利用し、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。

■ iR-ADV ／ 一部のimagePRESSシリーズでのファイアウォール設定画面

※設定手順については、本体同梱の取扱説明書を参照してください。

■ iRC ／ iR ／ imagePRESSシリーズでのIPアドレス範囲設定画面

※設定手順については、本体同梱の取扱説明書を参照してください。

複合機が持つ情報をパスワードで管理する

万が一、悪意のある第三者から不正アクセスを受けたとしても、複合機が持つさまざまな情報をパスワードで保護しておけば、情報漏えいによるリスクを大幅に軽減できます。キヤノンの複合機は、さまざまな情報がパスワードで保護できるようになっています。ここでご紹介する例以外の機能や情報においてもパスワードが設定できるものがあるので、必要に応じて適切に設定してください。

※各機能のパスワード設定手順については、本体同梱の取扱説明書を参照してください。
※各機能のパスワード設定は、本体操作パネルやリモートUIで設定できます。

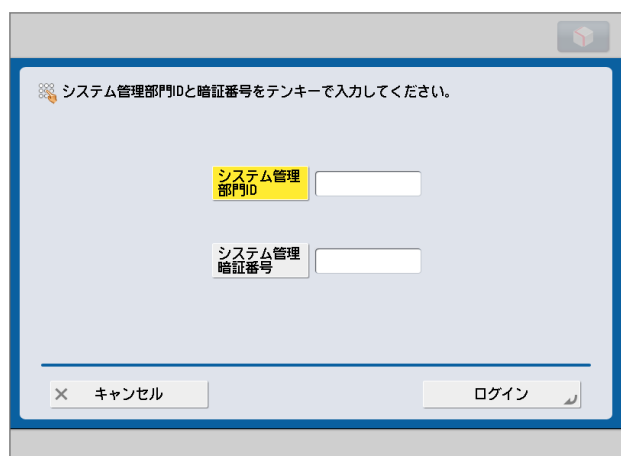
MEMO

リモートUI(User Interface)は、お手持ちのWebブラウザーからネットワークを経由して複合機にアクセスし、本機の状況の確認やジョブの操作、各種設定などができるソフトウェアです。本機の前に行かなくても、離れた場所からコンピューターで本機を管理できます。Webブラウザーで本機のIPアドレスまたはホスト名を指定すると、リモートUIのポータルページが表示されます。

※リモートUIの操作手順は本体同梱の取扱説明書を参照してください。

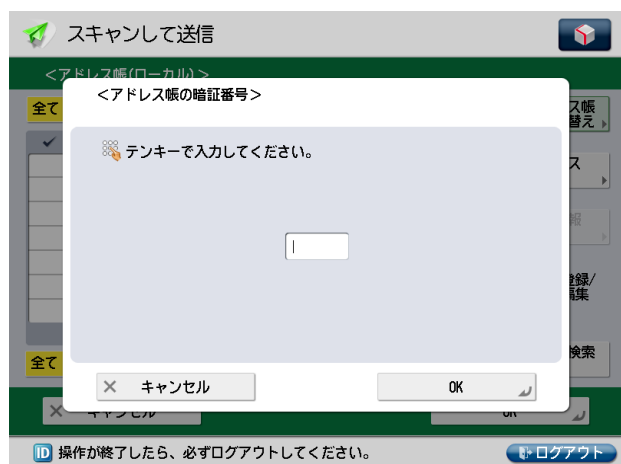
■ iR-ADV ／ 一部のimagePRESSシリーズでの各種画面

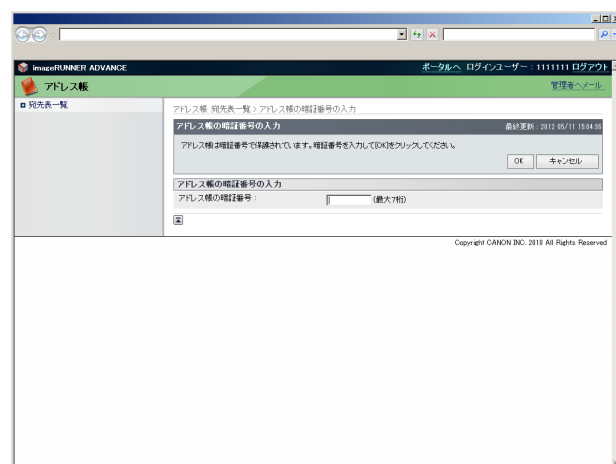
本体操作パネル

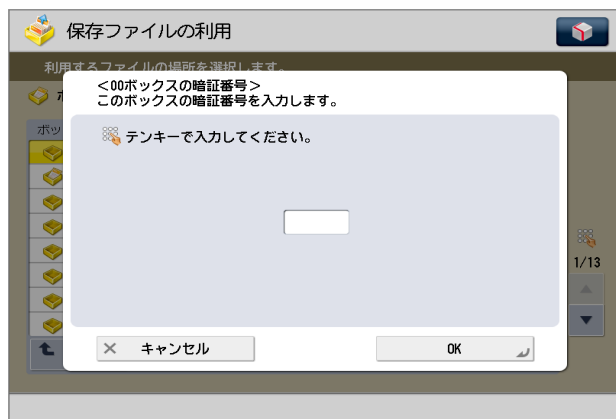
システム管理項目のパスワード入力画面

リモートUI

システム管理項目のパスワード入力画面

本体操作パネル

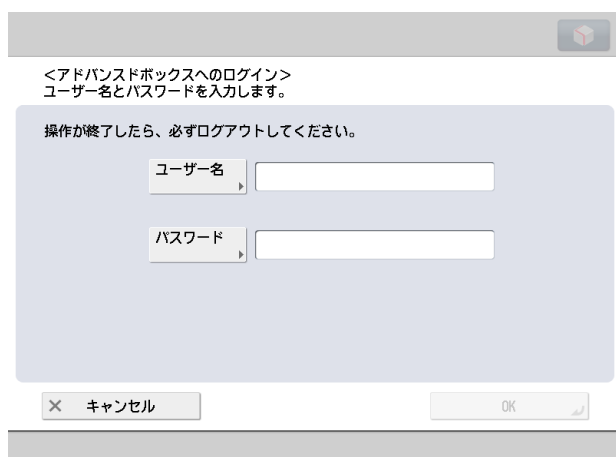
アドレス帳アクセス時のパスワード入力画面

リモートUI

アドレス帳アクセス時のパスワード入力画面

本体操作パネル

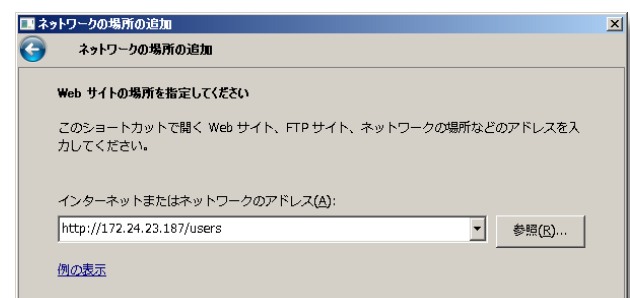
ボックスアクセス時のパスワード入力画面

リモートUI

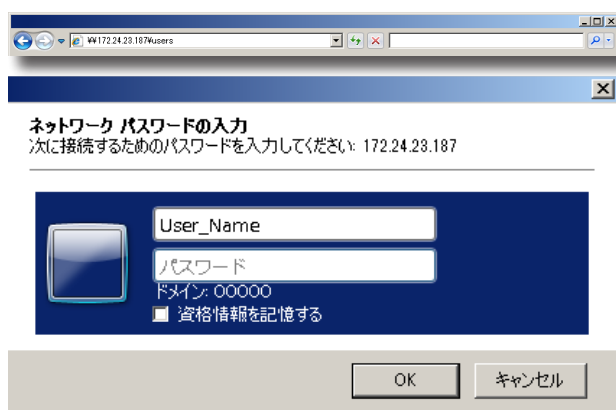
ボックスアクセス時のパスワード入力画面

本体操作パネル

アドバンスドボックスアクセス時パスワード入力画面

WebDAV

アドバンスドボックスアクセス時パスワード入力画面

WebDAVサーバーにアクセスする場合は、「http(s)://<本機のIPアドレスまたはホスト名>/<shareまたはusers>/<フォルダー名>」の形式で入力します。

SMB

アドバンスドボックスアクセス時のパスワード入力画面

SMBサーバーにアクセスする場合は、本機のホスト名またはIPアドレスに「¥share」または「¥users」をつけ、その次に「¥フォルダー名」を入力します。

MEMO

複合機はパスワードによる保護機能を備えていますが、パスワードの管理を行うことがセキュリティ対策において重要です。以下のポイントを参考に、パスワードを管理してください。

- 初期パスワードは必ず変更する
- 定期的にパスワードを変更する
- 第三者が推測しやすいパスワードを設定しない
- 不用意に第三者に教えない

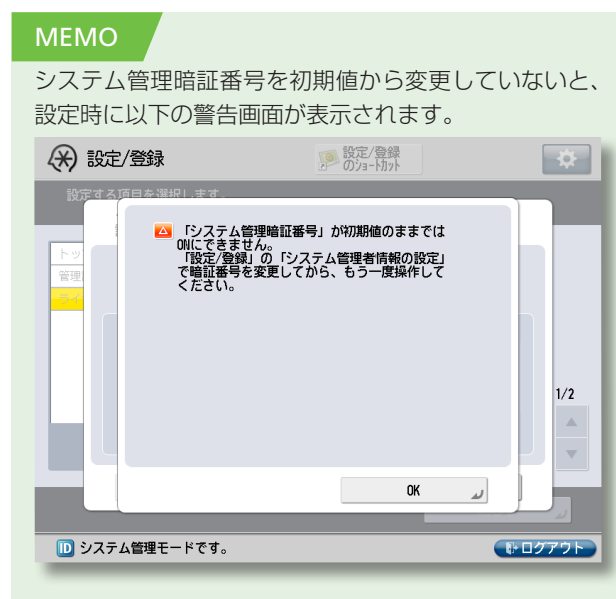
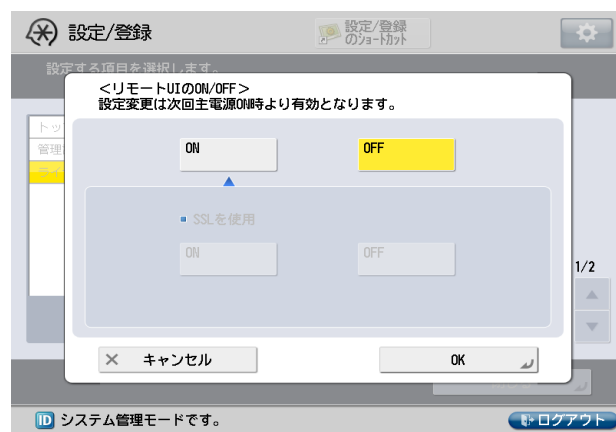
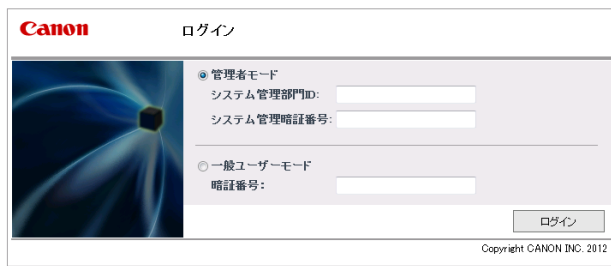
リモート UI の使用を制限する

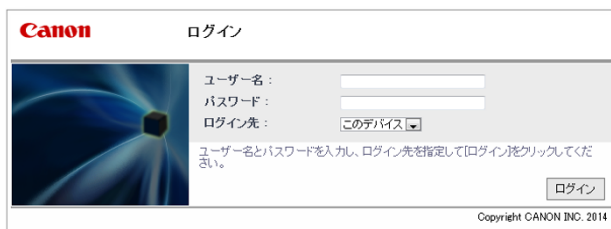
リモートUIには、使用を制限する機能が実装されセキュリティーを強化しています。

- リモートUIを利用するためには、システム管理暗証番号を初期値から変更する等の各種設定が必要となります。
- 一般ユーザーのリモートUIへのアクセス制限を設定できます。管理者権限、一般ユーザー権限のいずれの場合も、暗証番号（パスワード）の入力が必要となります。

■ iR-ADV ／ 一部のimagePRESSシリーズでのリモートUIのON/OFF設定画面

MEMO

システム管理暗証番号を初期値から変更していないと、設定時に以下の警告画面が表示されます。

※お使いの機種によっては、画面が異なる場合があります。

■ iR-ADV ／ 一部のimagePRESSシリーズでのリモートUIログイン画面

お使いの機種・設定により、ログイン画面が異なります。

ログイン画面①

管理者はアクセス時にシステム管理部門ID ／暗証番号の入力を、一般ユーザーはアクセス時に暗証番号の入力を求められます。

ログイン画面②

管理者・一般ユーザーに関わらず、アクセス時にユーザー名／パスワードが求められます。

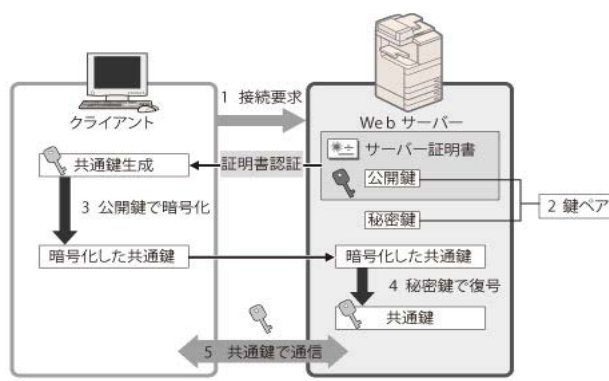
※現在お使いの製品で、本機能の対応については担当サービスにお問い合わせください。

SSL 暗号化通信を設定する

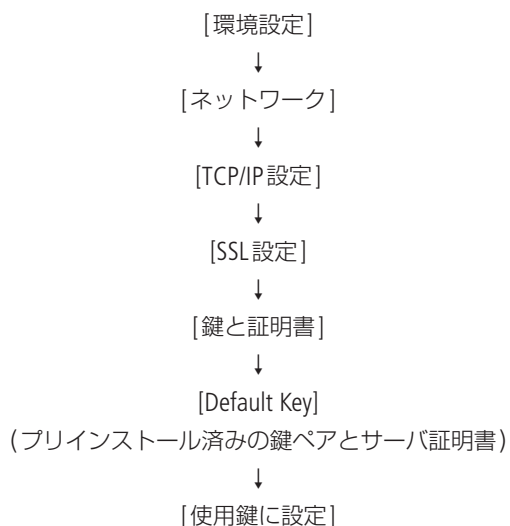
ユーザーがブラウザーを通してキヤノンの複合機にアクセスする際に、本機にサーバー証明書を導入することで、SSLによる安全な暗号化通信を実現できます。SSL通信ではサーバー証明書と公開鍵を利用して、ユーザーと本機の双方のみで使用できる共通鍵を互いに生成します。それにより、外部ネットワークからの不正アクセスを防ぐことができます。

※SSL通信の設定手順については、本体同梱の取扱説明書を参照してください。

SSL通信の仕組み（右図）

1. ユーザーのコンピューターから本機へアクセスするとき、SSLのサーバー証明書とサーバーの公開鍵を要求します。
2. 本機からユーザーのコンピューターへ証明書と公開鍵が送られます。
3. サーバーから受け取った公開鍵を使用して、コンピューター内で独自に生成した共通鍵を暗号化します。
4. 暗号化した共通鍵を本機に送ります。
5. 本機で秘密鍵を使用し、暗号化された共通鍵を復号する。
6. これによりユーザーのコンピューターと本機の双方で共通鍵を所有することになり、互いに共通鍵を使用してのデータのやり取りができるようになります。

■ iR-ADV ／ 一部のimagePRESSシリーズでのSSL設定画面

[環境設定]
↓
[ネットワーク]
↓
[TCP/IP設定]
↓
[SSL設定]
↓
[鍵と証明書]
↓
[Default Key]
（プリインストール済みの鍵ペアとサーバ証明書）
↓
[使用鍵に設定]

その他

■ リモートUI利用上での注意

Webブラウザーでプリンターのリモート UIを開いている時には、他のWebサイトにアクセスしないようにしてください。また、リモートUIで設定変更を行っているコンピューターから離席する場合や設定変更が終了した場合は、Webブラウザーを必ず終了してください。